CLAIMS

1. A method for carrying out an authentication process for authenticating a transaction with an entity (22) by means of a data processing apparatus (10), in which:

the entity (22) generates transaction data relating to the transaction, and

at least during the authentication process the data processing apparatus (10) has operatively associated with it a selected one of a plurality of authentication storage means (12) each for storing predetermined authentication information, the authentication storage means (12) being registrable with a common system (16),

the method including the step of carrying out the authentication process via a communications link with that system (16), the authentication process being carried out by authenticating means (102) incorporated in the system (16) and involving the use of the predetermined authentication information stored by the selected one authentication storage means (12) and the transaction data,

wherein in order to authenticate the transaction, the transaction data is transmitted between the data processing apparatus (10) and the system (16) via a transaction manager (14) implemented by the data processing apparatus, and the predetermined authentication information is also transmitted between the authentication storage means (12) and the system (16) via the transaction manager (14).

2. A method according to claim 1, in which the predetermined authentication information stored by each authentication storage means (12) corresponds to information which is used to authenticate a user of that authentication storage means (12) in relation to the system (16).

3. A method according to claim 1 or 2, wherein the system (16) is a telecommunications system.

4. A method according to claim 3, wherein the system (16) is a mobile and/or cellular telecommunications system.

5. A method according to claims 1,2,3 or 4, wherein each user is authenticated in the telecommunications system by means of the use of a smart card or subscriber identity module (e.g. SIM), and in which the authentication storage means (12) respective to that user corresponds to or simulates the smart card for that user.

6. A method according to claim 5, wherein the smart card or SIM authenticates the transaction when the smart card or SIM is operable in a terminal usable in a mobile and/or cellular telecommunications system.

7. A method according to claim 6, wherein the smart card or SIM is operable to authenticate the terminal in the mobile and/or cellular telecommunications system.

8. A method according to any preceding claim, in which the transaction is a

transaction involving use of the data processing functions of the data processing apparatus (10).

9. A method according to any preceding claim, in which each authentication storage means (12) is associated with a specific data processing apparatus (10).

10. A method according to any preceding claim, in which the authentication storage means (12) associated with the data processing apparatus (10) by being associated with data or software for use by that data processing apparatus (10).

11. A method according to claim 10, in which the authentication storage means (12) is incorporated on a data carrier for the data or software.

12. A method according to any preceding claim, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

13. A method according to any preceding claim, including the step of levying a charge for the transaction when authenticated.

14. A method according to claim 13, in which the step of levying the charge is carried out by the said system.

15. A method according to any preceding claim, in which the data processing apparatus is a personal computer (10).

16. A method according to any preceding claim, wherein the authentication storage means (12) communicates wirelessly to authenticate the transaction.

17. A method according to any preceding claim, including operatively coupling the authentication storage means (12) to a carrier (32).

18. A method according to claim 17, including operatively coupling the carrier (32) to the data processing apparatus (10) for enabling data communication between said authentication storage means (12) and said data processing apparatus (10) and/or said system (16).

19. A method according to claim 18, wherein the carrier (32) is operatively coupled to the data processing apparatus (10) by a wireless link.

20. A method according to any of claims 17 to 19, wherein the authentication storage means (12) is removably coupled to the carrier (32).

21. A method according to any one of claims 17 to 20, wherein the carrier (32) controls access to the predetermined authentication information.

22. A method according to claim 21, comprising using said carrier (32) to obtain security data independently of the data processing apparatus (10), and analysing the security data for determining whether to allow access to the predetermined information.

23. A method according to claim 22, wherein the security data is obtained by alphanumeric data entry means.

24. A method according to claim 22 or 23, wherein the alphanumeric data entry means comprises a keypad (46).

25. A method according to claim 22,23 or 24, wherein the security data comprises a Personal Identification Number (PIN) and the analysing step compares the PIN obtained

by the security data entry means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

26. A method according to any one of claims 21 to 25, comprising displaying security information.

27. A method according to any one of claims 21 to 26, wherein communication with the data processing apparatus (10) is controlled by a data processing module (36).

28. A method according to claim 27, wherein the data processing module (36) of the carrier (32) is configured for communicating with a corresponding data processing module (38) of the data processing apparatus (10).

29. A method according to claim 28, wherein communication between the authentication storage means (12) and the data processing apparatus (10) is performed via the respective data processing modules (36,38).

30. A method according to claim 27,28 or 29, wherein the data processing module (36) of the carrier (32) decrypts encrypted data received from the data processing module (38) of the data processing apparatus (10).

31. A method according to claim 27,28,29 or 30, wherein the data processing module (36) of the carrier (32) encrypts data transmitted to the data processing module (38) of the data processing apparatus (10).

32. A method according to claim 30 and 31, wherein the respective data processing modules (36,38) comprise a key (40,42) for allowing encryption and/or decryption of data.

33. A method according to claim 32, wherein the key (40,42) comprises a shared secret key for each of the respective data processing modules (36,38).

34. A method according to any one of claims 17 to 33, wherein the carrier (32) is operatively coupled to a plurality of authentication storage means (12) for respectively enabling the said authentication process and one or more other authentication processes.

35. A method according to claim 34, wherein said one or more other authentication processes are carried out via a communications link with the system (16).

36. A method according to any preceding claim, including routing communications between the authentication storage means (12) and the system (16) via the transaction manager (14).

37. A method according to any preceding claim, wherein the transaction manager (14) is implemented by the data processing apparatus.

38. A method according to any preceding claim, wherein the transaction manager (14) detects the operative coupling of the authentication storage means (12).

39. A method according to claim 36,37 or 38, wherein the transaction manager (14) transmits data relating to an authenticated transaction to the entity (22) to which that transaction relates.

40. A method according to claim 39, wherein the entity (22) is controlled by the data processing means (10).

41. A method according to claim 39, wherein the entity (22) is controlled by the system (16).

42. A method according to claim 39, wherein the entity (16) is independent of the data processing means (10) and/or the system (16).

43. A method according to claim 39,40 or 41, wherein the data related to the transaction with the entity is provided under the control of an application (17) provided by the data processing apparatus (10).

44. A method according to any one of claims 1 to 14 or 16 to 43, wherein the entity (22) includes means for providing goods and/or services in response to the authentication.

45. A method according to any one of claims 39 to 44 wherein, following authentication of a transaction by the authentication means (102) of the system (16), a security token is generated by the system and which includes data relating to the authenticated transaction, and wherein the security token is made available to the entity for facilitating performance of the transaction.

46. A method according to claim 45, wherein the security token includes data relating to the entity (22).

47. A method according to claim 46, wherein the security token includes data rendering the security token only usable to facilitate performance of a transaction with a predetermined entity.

48. A method according to claim 47, wherein the security token includes data for facilitating the entity obtaining payment for the transaction.

49. A method according to any preceding claim, wherein the system (16) stores user data relating to a user of the system with which the authentication storage means (12) is

associated.

50. A method according to any one of claims 39 to 49, wherein the user data is selectively made available to the entity (22).

51. A method according to claim 50, wherein the user data is provided in response to an indication from the entity (22) that the entity has received a security token relating to the user.

52. Data processing apparatus (10) in combination with a selected one of a plurality of authentication storage means (12) each for storing predetermined authentication information relating to the carrying out of an authentication process for authenticating a transaction with an entity (22) by means of the data processing apparatus (10), the entity (22) being operable to generate transaction data relating to the transaction, and the authentication storage means (12) all being registrable with a common system (16), the authentication storage means (12) when operatively associated with the data processing apparatus (10) being operative to carry out the authentication process via a communications link with that system (16), the authentication process being carried out by authenticating means (102) incorporated in the system (16) and involving the use of the predetermined authentication information stored by the selected one authentication storage means (12), wherein in order to authenticate the transaction, the transaction data is transmitted between the data processing apparatus (10) and the system (16) via a transaction manager (14) implemented by the data processing apparatus (10), and the predetermined authentication information is also transmitted between the authentication storage means (12) and the system via the transaction manager (14).

53. Apparatus according to claim 52, in which the predetermined authentication information stored by each authentication storage means (12) corresponds to information which is used to authenticate a user of that authentications storage means (12) in relation

to the system (16).

54. Apparatus according to claim 52 or 53, wherein the system is a telecommunications system (16).

55. Apparatus according to claim 54, wherein the system is a mobile and/or cellular telecommunications system (16).

56. Apparatus according to claim 53,54 or 55, in which each user is authenticated in the telecommunications system by means of the use of a smart card or subscriber identity module (e.g. SIM), and in which the authentication storage means (12) respective to that user corresponds to or simulates the smart card for that user.

57. Apparatus according to claim 56, wherein the smartcard or SIM is operable in a terminal usable in a mobile and/or cellular telecommunication system to authenticate the transaction.

58. Apparatus according to claim 57, wherein the smartcard or SIM is operable to authenticate the terminal in the mobile and/or cellular telecommunication system.

59. Apparatus according to any one of claims 52 to 54, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus (10).

60. Apparatus according to any one of claims 52 to 59, in which the authentication storage means (12) is specific to the data processing apparatus (10).

61. Apparatus according to any one of claims 52 to 60, in which the authentication process involves the sending of a message and the generation of a response dependent on

the message and the predetermined information.

62. Apparatus according to any one of claims 52 to 61, including means for levying a charge for the transaction when authorised.

63. Apparatus according to claim 62, in which the means for levying the charge is part of the common system (16).

64. Apparatus according to any one of claims 52 to 63, in which the data processing apparatus (10) is a personal computer.

65. Apparatus according to any one of claims 52 to 64, comprising means for enabling the authentication storage means (12) to communicate wirelessly to authenticate the transaction.

66. Apparatus according to any one of claims 52 to 65, wherein a carrier (32) is provided for the authentication storage means (12) and the authentication storage means is operatively couplable to the carrier (32).

67. The apparatus of claim 66, wherein the carrier (32) is operatively couplable to the data processing apparatus (10) for enabling data communication between the authentication storage means and the data processing apparatus (10) and/or the system (16).

68. Apparatus according to claim 67, including means for allowing wireless communication between the carrier (32) and the data processing apparatus (10).

69. Apparatus according to claim 66, 67 or 68, including means for removably coupling the carrier (32) to the authentication storage means (12).

70. Apparatus according to any one of claims 66 to 69, wherein the carrier (32) includes means for controlling access to the predetermined authentication information.

71. Apparatus according to claim 70, wherein the carrier (32) includes means (46) for obtaining security data independently of the data processing apparatus (10) and means for analysing the security data for determining whether to allow access to the predetermined information.

72. Apparatus according to claim 71, wherein the carrier (32) comprises alphanumeric data (46) entry means for allowing the security data to be obtained.

73. Apparatus according to claim 72, wherein the alphanumeric data entry means (46) comprises a keypad.

74. Apparatus according to claim 71, 72 or 73, wherein the security data comprises a personal identification number (PIN) and the analysing means is operable to compare the PIN obtained by the security data entry means with a PIN stored on the authentication storage means (12) and for only allowing access to the predetermined information when the respective PINs match.

75. Apparatus according to any one of claims 70 to 74, wherein the carrier (32) includes means (48) for displaying security information.

76. Apparatus according to any one of claims 70 to 75, wherein the carrier (32) comprises a data processing module (36) for controlling communication with the data processing apparatus (10).

77. Apparatus according to claim 76, wherein the data processing module (36) of the

carrier (32) is configured for communicating with a corresponding data processing module (38) of the data processing apparatus (10).

78. Apparatus according to claim 77, wherein communication between the authentication storage means (12) and the data processing apparatus (10) is performed via the respective data processing modules (36,38).

79. Apparatus according to claim 76, 77 or 78, wherein the data processing module (36) of the carrier (32) includes means for decrypting encrypted data received from the data processing module (38) of the data processing apparatus (10).

80. Apparatus according to claim 76,77,78 or 79, wherein the data processing module (36) of the carrier (32) encrypts data transmitted to the data processing module (38) of the data processing apparatus (70).

81. Apparatus according to claim 79 or 80, wherein the respective data processing modules comprise a key (40,42) for allowing encryption and/or decryption of data.

82. Apparatus according to claim 81, wherein the key (40,42) comprises a shared secret key for each of the respective data processing modules (36,38).

83. Apparatus according to any one of claims 66 to 82, wherein the carrier (32) includes means for operatively coupling the carrier to a plurality of authentication storage means (12) for respectively enabling the said authentication process and one or more other authentication processes to be performed.

84. Apparatus according to claim 83, wherein the said one or more other authentication processes are carried out via a communications link with the system (16).

85. Apparatus according to any one of claims 52 to 84, wherein data communications between the authentication storage means (12) and the system (16) are routed via the transaction manager (14).

86. Apparatus according to any one of claims 52 to 85, wherein the transaction manager (14) is implemented by the data processing apparatus (10).

87. Apparatus according to any one of claims 52 to 86, wherein the transaction manager (14) is operable to detect the operative coupling of the authentication storage means (12) to the data processing means (10).

88. Apparatus according to any one of claims 52 to 87, wherein the transaction manager (14) is operable to transmit data relating to an authenticated transaction to the entity (22) to which that transaction relates.

89. Apparatus according to claim 88, wherein the entity (22) is controlled by the data processing means (10).

90. Apparatus according to claim 89, wherein the entity (22) is controlled by the system (16).

91. Apparatus according to claim 89, wherein the entity (22) is independent of the data processing (10) means and/or the system (16).

92. Apparatus according to claim 88,89 or 90, wherein an application (17) is provided by the data processing apparatus (10) which controls the provision of data related to the transaction to the entity (22).

93. Apparatus according to any one of claims 52 to 63 or 65 to 92, wherein the entity

(22) includes means for providing goods and/or services in response to the authentication.

94. Apparatus according to any one of claims 88 to 93, wherein the system (16) includes means (102) for generating a security token in response to authentication of a transaction by the authentication means (102) of the system (16), which security token includes data relating to the authenticated transaction, such that the security token facilitates performance of the transaction when the security token is made available to the entity.

95. Apparatus according to claim 94, wherein the security token includes data relating to the entity (22).

96. Apparatus according to claim 95, wherein the security token includes data rendering the security token only usable to facilitate performance of a transaction with a predetermined entity.

97. Apparatus according to claim 96, wherein the security token includes data for facilitating the entity of obtaining payment for the transaction.

98. Apparatus according to any one of claims 52 to 97, wherein the system (16) stores user data relating to a user of the system with which the authentication storage means (12) is associated.

99. Apparatus according to any one of claims 88 to 98, wherein the system (16) includes means for selectively making available user data to the entity.

100. Apparatus according to claim 99, wherein the user data is provided in response to an indication from the entity that the entity has received a security token relating to the user.

101. A device (32) for coupling to data processing apparatus (10) for enabling an authentication process involving the use of separate authenticating means (102), the device (32) being configured to provide a plurality of separately activatable authentication information records for use in the authentication process, the authentication information records being registered with a system (16) including the authenticating means (102), the device (32) being responsive to an input message for deriving a response dependent on the input message and on the activated authentication information record for enabling the authenticating means (102) to carry out the authentication process via a communication link with the authenticating means (102) in the said system (16) whereby to authenticate a transaction.

102. The device of claim 101, including means for receiving a smart card or SIM which carries said plurality of authentication information records

103. The device of claim 101, including means for receiving a plurality of smart cards or SIMs, each of which carries one of said plurality of authentication information records.

104. The device of claim 101, including means for releasably coupling one or a plurality of smart cards or SIMs thereto, the authentication information records being stored on the smart card(s) or SIM(s).

105. The device of claim 101, including means for receiving one or a plurality of smart cards or SIMs and for permanently coupling the smart card(s) or SIM(s) to the device.

106. The device of claim 101, including a data store for storing said plurality of separately activatable authentication information records.

107. The device of any of claims 101 to 106, wherein the plurality of authentication

information records are selectively activated in response to a user input.

108. The device of claim 107, wherein the user input is provided by activation of a switch.

109. The device of any of claims 101 to 106, wherein the plurality of authentication information records are selectively activated in response to a signal received from the data processing device.

110. An authentication system for authenticating transactions of users registered with that system to enable a transaction with another system (22) to be authenticated, the authentication system including authentication means (102) for sending an authentication message in response to an authentication request from a subscriber and for receiving and analysing a response thereto to determine if the received response corresponds to an expected response to authenticate the identity of the user; and security token generating means (102) for generating a security token for use in performing a transaction with the other system (22).

111. The system of claim 110, wherein the security token includes data indicative of the identity of the user.

112. The system of claim 110 or 111, wherein the security token includes data indicative of the nature of the transaction.

113. The system of claim 110,111 or 112, including means (102) for receiving a returned security token and for analysing the returned security token to determine its integrity and for providing a service in response to receipt of the returned security token.

114. The system of claim 113, wherein the service is the processing of a payment

associated with the transaction.

115. The system of claim 110,111,112,113 or 114, including a register for storing data relating to a user for use in performing transactions.

116. The system of claim 115, including means for transmitting the user data in response to a request from the user.

117. The system of claim 115, including means for transmitting the user data in response to receipt of a returned security token.

118. The system of claim 115, 116 or 117, wherein the register stores for each user separate data records for each of a plurality of other services with which the user performs transactions, and wherein only user data for a particular service is provided in response to a request for user data.

119. The system of claim 118 when dependent on claim 117, wherein the returned security token in analysed to determine to which service it relates, and in response thereto user data for that service is provided to that service.

120. A system for storing user data for use in performing transactions with a plurality of service providers, wherein for each user a plurality of data records are stored for use when performing transactions with respective service providers, and wherein only a data record relevant to a particular service provider is made available in response to a request on behalf of that service provider.

121. The system of claim 120, including means for authenticating a request for user data on behalf of a service provider.

122. A data packet for use in authenticating and performing a transaction between a client and a product or service provider, the data packet including data indicative of the product or service provider identity such that the data packet is only useable to authenticate and perform a transaction with that product or service provider.

123. The data packet of claim 122, wherein the data packet includes data indicative of the client identity such that the data packet is only useable to authenticate and perform a transaction with that client.

124. An authentication system for authenticating transactions between a client and a product or service provider, including means for generating a data packet according to claim 122 or 123 and means for transmitting the data packet to the service provider.

125. A method of facilitating transactions between a plurality of users registered with an authentication system (16) and plurality of product or service providers (22), the method including:

providing each user with authentication storage means (12) storing predetermined authentication information, each authentication storage means being coulpleable to data processing apparatus (10) for data exchange therewith;

generating in response to a request, made using data processing apparatus (10), from a user to a product or service provider a transaction request data packet including data indicative of the identity of the user and the identity of the product or service provider (22);

transmitting the transaction request data packet to the authentication system (102) via the data processing apparatus (10);

analysing in the authentication system (102) the transaction request data packet and extracting therefrom the identity of the user;

transmitting from the authentication system (102) an authentication request signal to the user's authentication storage means (12) via the data processing apparatus (10);

receiving via the data processing apparatus (10) a response from the user's authentication storage means at the authentication system (102);

analysing said response at the authentication system (102) to determine whether said response corresponds to an expected response with reference to knowledge of said predetermined authentication information for that user;

generating an authentication token and providing this to the product or service provider (22) via the data processing apparatus (10), the authentication token indicating to the product and service provider that the user is authenticated by the authentication system (102).

126. The method of claim 125, wherein the authentication token includes data indicative of the product or service provider that generated the transaction request data packet corresponding to the authentication token.

127. The method of claim 125 or 126, wherein the authentication token includes data indicative of the user.

128. The method of claim 125,126 or 127, including receiving from the service provider (22) at the authentication system (102) a request for payment token, including the authentication token to which it relates, checking the validity of the authentication token prior to authorising a payment to the product or service provider from the user's account with the authentication system (102).

129. A method for carrying out an authentication process for authenticating a subsequent transaction by any one of a plurality of users with an entity (22) by means of data processing apparatus (10), in which:

the entity (22) generates transaction data relating to the transaction, and

during the authentication process the data processing apparatus (10) has operatively associated with it a selected one of a plurality of authentication storage means

(12) respective to the users, each authentication storage means (12) storing predetermined authentication information and being registerable with a common telecommunications system (16) for which the users have respective telecommunications terminals,

the method including the step of carrying out the authentication process via a communications link with the common telecommunications system (16), the authentication process being carried out by authenticating means (102) incorporated in the telecommunications system (16) and involving the use of the predetermined authentication information stored by the selected one authentication storage means (12), the predetermined authentication information stored by each authentication storage means (12) corresponding to information which is used to authenticate that user's telecommunications terminal in relation to the telecommunications system (16) but the authentication process for authenticating the transaction by that user with the data processing apparatus (10) not requiring use of that user's telecommunications terminal nor requiring the telecommunications terminal to be actually authenticated by that information in relation to the telecommunications system (16),

wherein in order to authenticate the transaction, the transaction data is transmitted between the data processing apparatus (10) and the system (16) via a transaction manager (14) implemented by the data processing apparatus (10), and the predetermined authentication information is also transmitted between the authentication storage means (12) and the system (16) via the transaction manager (14).